PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 4 :
H04N 7/167, H04L 9/00

A1

(11) International Publication Number: WO 86/ 07224

(43) International Publication Date: 4 December 1986 (04.12.86)

(21) International Application Number: PCT/US86/00801

(22) International Filing Date: 21 April 1986 (21.04.86)

(31) Priority Application Number: 737,599

(32) Priority Date: 24 May 1985 (24.05.85)

(33) Priority Country: US

(71) Applicant: SCIENTIFIC ATLANTA, INC. [US/US]; One Technology Parkway, Box 105600, Atlanta, GA 30348 (US).

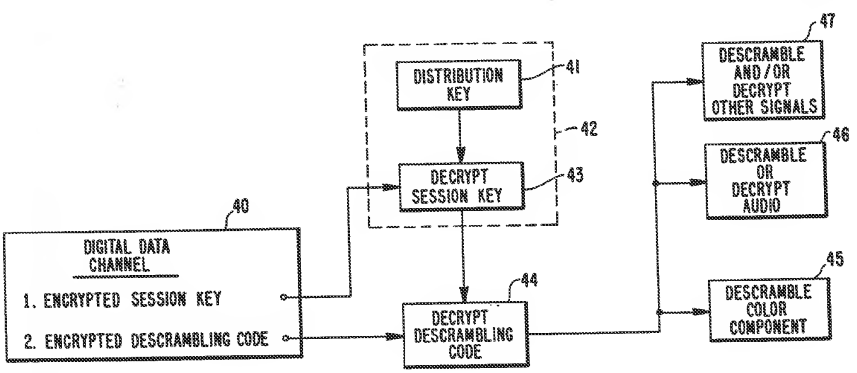
(72) Inventor: LUCAS, Keith ; 41 Beaufort Hills Road, Oak Ridges, Ontario LOG 1PO (CA).

(74) Agents: PETERSON, Thomas, L. et al.; Banner, Birch, McKie & Beckett, One Thomas Circle, N.W., Washington, DC 20005 (US).

(81) Designated States: AT, AT (European patent), AU, BB, BE (European patent), BG, BR, CH, CH (European patent), DE, DE (European patent), DK, FI, FR (European patent), GB, GB (European patent), HU, IT (European patent), JP, KP, KR, LK, LU, LU (European patent), MC, MG, MW, NL, NL (European patent), NO, RO, SD, SE, SE (European patent), SU.

Published
With international search report.

(54) Title: METHOD AND APPARATUS FOR SCRAMBLING AND DESCRAMBLING TELEVISION SIGNALS



(57) Abstract

A method and apparatus for descrambling a television signal using a three tier encryption technique for the code used to descramble the signal. At the transmitter, a distribution key (41) is used to encrypt a session key. The encrypted session key (40.1) is transmitted in the digital data channel (40) of the television signal. The session key is also used to encrypt the descramble code (40.2) which is also transmitted in the data channel (40) of the television signal. At the receiver (42) the encrypted session key (43) is decrypted using a distribution key (41). The decrypted session key (43), is in turn used to decrypt the descramble code (44). The descramble code may then be used to descramble and/or decrypt other signals (45, 46, 47) in the receiver.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GA**	Gabon	**MR**	Mauritania
AU	Australia	**GB**	United Kingdom	**MW**	Malawi
BB	Barbados	**HU**	Hungary	**NL**	Netherlands
BE	Belgium	**IT**	Italy	**NO**	Norway
BG	Bulgaria	**JP**	Japan	**RO**	Romania
BR	Brazil	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SN**	Senegal
CH	Switzerland	**LI**	Liechtenstein	**SU**	Soviet Union
CM	Cameroon	**LK**	Sri Lanka	**TD**	Chad
DE	Germany, Federal Republic of	**LU**	Luxembourg	**TG**	Togo
DK	Denmark	**MC**	Monaco	**US**	United States of America
FI	Finland	**MG**	Madagascar		
FR	France	**ML**	Mali		

METHOD AND APPARATUS FOR SCRAMBLING AND DESCRAMBLING TELEVISION SIGNALS

BACKGROUND OF THE INVENTION

The present invention relates generally to the field of communication systems and, more particularly, is directed to a method and apparatus for scrambling and descrambling television signals in a subscription television system.

Subscription television systems have gained widespread acceptance as an efficient way of providing a vast selection of information and entertainment programming to the public. However, the cost of a good quality system is high. Thus, care must be taken to ensure an adequate financial return to the broadcaster for maintenance of the system. Toward that end, many broadcasters have turned to scrambling the broadcast signal to induce payment from those desiring the service. Only subscribers to the system are provided with a decoder for descrambling the signal. Moreover, many decoders are designed so that the signal is descrambled only when the subscriber's account is in good standing.

Many scrambling methods and apparatus rely on the fact that television signals are produced and displayed as a result of a line scanning process. The picture information is scanned using a progressive series of horizontal lines which are transmitted sequentially in time. The transmitted signal is a continuous analogue of the brightness intensity corresponding to each point of the line. Such a signal is shown in Figure 1 from which it may be seen that in a series of standard lines, any two adjacent active line periods (periods during which video information is transmitted) are separated by a

period in which no video information is transmitted. This latter period is known as the horizontal line blanking interval and is introduced to allow the scanning device in the television receiver to reset to the line-start position.

In typical color television signals, the active line period includes one signal which simultaneously represents the instantaneous values of three independent color components. The method by which the three color components are coded into one signal is standardized throughout North America, Canada and Japan. This method is known as the NTSC standard. Alternative standards known as PAL and SECAM have been adopted in other countries but these standards have the same basic format as the NTSC standard, including a line blanking interval and an active line period in each scan line.

Other types of analogue video signals which are particularly adapted for transmission by satellite and cable, and which lead to improved picture quality in comparison with existing standards, are presently being studied. Such signals are of particular importance to the subscription television field and are based on a time multiplex of the three independent color components during the active line periods of the scan line. Instead of coding the three components into one signal using the NTSC, PAL or SECAM standard, the components are converted to digital form and sent sequentially using a time-compression technique. One version of this type of signal is known as Multiplexed Analogue Components (MAC). Signals generated by a time compression technique also adhere to the same basic format as the NTSC, PAL and SECAM standards, including the presence of a line blanking interval and an active line period in each scan line. When a MAC signal is employed, digital data may be transmitted during the line blanking interval as shown by the dotted lines in Figure 2. Thus, the audio portion of the signal may be converted to digital form and transmitted during the line blanking interval as digital data. Accordingly, the line blanking interval is ofter referred to as the "data

channel" and can include several multiplexed data signals. The color components, audio signals and any signals in the data channel can be collectively referred to as the intelligence portion of the television signal.

In scrambling a television signal, selected parameters of the analogue video components of the signal are modified in accordance with pseudo-random scrambling codes. The codes can be signaled to the television receiver in the data channel of the signal and are used by a decoder at the receiver to descramble the video components for reconstruction to the appropriate format for viewing. The data channel may also be securely encrypted to further frustrate reception of the signal by unauthorized persons.

Though the terms "encryption" and "scrambling," and their converse "decryption" and "descrambling," are often used interchangeably, there is a distinction between them. Encryption and decryption are applied to digital data signals and scrambling and descrambling are applied to analogue signals. This distinction is drawn because of the fundamental difference between digital and analogue signals. Digital signals are defined at the bit level where each bit is independent of its neighboring bits. Any encoding, transformation or inversion of the data bits which make up the signal does not affect the signal's transmission characteristics at the bit level. Thus, an encrypted digital signal contains all of the information present in the original signal and may be precisely restored to the original signal by decryption. Analogue signals, on the other hand, cannot be modified or changed without affecting their transmission characteristics. For example, changing the value of a point on the waveform of an analogue signal without reference to neighboring points on the waveform increases the bandwidth of the signal. Thus, the modified signal requires a wider bandwidth for accurate transmission. Therefore when scrambling an analogue signal, parameters must be selected which result in the least amount of change in transmission characteristics of the signal.

Numerous methods may be used to scramble a television signal by modifying the analogue color components of the signal. Such methods include modifying the amplitude of the color components, modifying the time at which the color components are transmitted and modifying both the amplitude and transmission time of the color components. Each modification is, of course, done in accordance with a prescribed pattern which may be transmitted to the receiver in the data channel of the television signal. An example of scrambling a television signal by modifying the time at which the color components are transmitted is disclosed in commonly assigned U.S. Patent Application Serial No. 507,765 entitled "Encryption and Decryption (Scrambling and Descrambling) of Video Signals" filed June 24, 1983. Said application is incorporated herein by reference. The color components could also be encrypted while being converted to digital form for time-compressed transmission, as for example in a MAC television signal. Such an encryption method is disclosed in commonly assigned U.S. Patent Application Serial No. 736,301 entitled "Method and Apparatus for Creating Encrypted and Decrypted Television Signals" filed May 21, 1985. This application is also incorporated herein by reference. Moreover, the audio component of the television signal can be scrambled in its analogue form or can be converted to digital form, encrypted and transmitted in the data channel.

In typical encryption systems, the bit configuration of the digital data signal to be encrypted is modified according to a pattern which is determined at the transmitter. The pattern generally is a member of a large class of similar patterns such that discovery of the pattern through exhaustive search is extremely unlikely. A precise description of the pattern used for encryption is delivered to a decoder in designated receivers which then is able to recover the original distribution. The description of the pattern is known in the art as the "encryption key" and the process of informing designated users of the encryption key, or more appropriately the "decryption key," is known as "key

distribution." The decryption key is derived from the encryption key and permits the encrypted information to be returned to its original form.

Numerous encryption codes are available in the art for the secure encryption of digital data. Integrated circuit devices presently exist for certain algorithms which execute high speed encryption and decryption sufficient for the data channel of a television signal. One such algorithm which has gained acceptance as being difficult to break is the Data Encryption Standard (DES) adopted by the U.S. National Bureau of Standards. Other algorithms are also available, the only requirement being that the data channel be essentially impossible to decrypt in the absence of the decryption key.

Since an encrypted data channel containing descrambling codes for the color components of a television signal, and perhaps audio information as well, is ususally encrypted in only one way, the decryption key (i.e., the reverse of the encryption key) for decrypting the channel must be common to all users. Use of a common decryption key, however, requires that means be provided to prevent circulation of the decryption key to those who are not subscribers to the system or to subscribers who are not presently in good standing.

SUMMARY OF THE INVENTION

It is, therefore, an object of the present invention to provide a method and apparatus for securely scrambling a television signal.

It is a further object of the present invention to encrypt the scrambling codes used to scramble a television signal in a manner that cannot be detected by unauthorized recipients of the television signal.

The use of a common decryption must be distributed in such a manner that unauthorized recipients cannot receive the key. One such way of providing this security is to change the decryption key at short intervals (say for example, every minute), thereby forcing an unauthorized user of the service to maintain a permanent link with an authorized user so that he may continuously receive the updated

decryption key. A second way of fouling unauthorized reception of the decryption key is to perform a secondary encryption of the decryption key and to integrate the decryption key acquisition system at the receiver with data channel decryption in a single device which is difficult to copy.

The method and apparatus for securely scrambling a television signal in accordance with the present invention comprises a three-tier encryption technique. At the television transmitter, a distribution key is used to encrypt a session key. The distribution key is unique for each subscriber and is held constant for long periods of time. The session key, however, is changed periodically, as for example, weekly or monthly. The encrypted session key is then transmitted in the digital data channel of the television signal. The session key is also used to encrypt a descramble code. The descramble code includes a plurality of keys which are used in the receiver to descramble or decrypt various signals in the receiver, such as the scrambled video components and/or audio signals. The descramble code is also changed periodically, e.g., four times per second in order to provide additional security. The encrypted descramble code is then transmitted in the data channel of the television signal.

At the receiver, the encrypted session key is decrypted by a distribution key so that the session key can be used to dec : the encrypted descramble code. The descramble code may then be ed to descramble or decrypt other signals in the receiver, such as the scrambled video components and/or audio signals.

In another embodiment of the present invention, a validation code is also transmitted in the data channel of the television signal. The validation code received by the receiver is compared to a locally derived validation code which is developed from the decrypted session key. When the two validation codes match, the decrypted session key is permitted to decrypt the descramble code. The decrypted descramble code may then be used to decrypt and/or descramble other signals in the receiver.

BRIEF DESCRIPTION OF THE DRAWINGS

Figures 1 and 2 are graphical representations of a line scanned television signal.

Figure 3 is a block diagram of one embodiment of a system for encrypting the code used to descramble and/or decrypt the intelligence portion of a television signal in accordance with the present invention.

Figure 4 is a block diagram of one embodiment of a system for decrypting the code used to descramble and/or decrypt the intelligence portion of a television signal in accordance with the present invention.

Figures 5, 6 and 7 are block diagrams of other embodiments of a system for decrypting the code used to descramble and/or decrypt the intelligence portion of a television signal in accordance with the present invention.

Figure 8 is a block diagram of one example of a subscription television decoder.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figures 3 and 4 are block diagrams of one embodiment of a system for scrambling television signals in accordance with the present invention. Figure 3 illustrates encryption at the transmitter end and Figure 4 illustrates decryption at the receiver end. As shown in Figure 3, a session key 30 is encrypted in block 33 with a distribution key 32. The distribution key is unique for each subscriber and is held constant for long periods of time. The session key, on the other hand, is changed at predetermined intervals, e.g., weekly or monthly. The encrypted session key is then transmitted in the digital data channel of the television signal. The session key is also used to encrypt a descrambling code 31. The descrambling code includes keys for descrambling and/or decrypting various signals in the receiver. These signals may include the scrambled video components of the television signal, scrambled or encrypted audio signals and/or other signals which may require descrambling or decryption at the receiver. The encrypted descrambling code is also transmitted in the digital data

channel of the television signal. The descrambling code may also be regularly updated, e.g., four times per second, in order to provide further security.

With respect to Figure 4, block 40 represents the received digital data channel of the television signal which includes the encrypted session key and the encrypted descrambling code as shown in Figure 3. The encrypted session key is provided to block 43 along with a distribution key 41. The distribution key is assigned to subscribers in return for a paid subscription to the system. The key is unique to each individual subscriber, or is part of a set of keys large enough to prevent key swapping. Distribution key 41 may be the same as or derived from distribution key 32 shown in Figure 3. The encrypted session key is transmitted in the data channel by the television transmitter individually for each distribution key 41 in use.

Distribution key 41 is fixed for long periods of time and is maintained secret from the subscriber. One such way of maintaining the distribution key in confidence is to build it inside a custom integrated circuit as indicated by reference No. 42 which also executes session key decryption as shown in block 43. The digital bit pattern of the distribution key is also made long enough to prevent its discovery through exhaustive search. The encrypted session key is decrypted in block 43 by the distribution key and is supplied to block 44 along with the encrypted descrambling code from the data channel. The descrambling code is decrypted in block 44 by the now decrypted session key and is then available for descrambling or decrypting other signals such as the analogue color components of the television signal as shown in block 45, the audio portion of the television signal as shown in block 46 and any other signals in the receiver which may require descrambling or decryption as shown in block 47. Thus, the present invention provides three tiers of encryption and decryption before the scrambled or encrypted signal is returned to its original form.

Figure 5 is a further embodiment of the present invention with respect to decryption at the receiver end. Similar reference numbers are used to identify corresponding elements shown in Fiugre 4. In this embodiment, the audio portion of the television signal is encrypted and transmitted in the data channel. The audio and descramble code are decrypted in block 44 using the decrypted session key from block 43 as described above.

A further embodiment of the present invention with respect to decryption at the receiver end is shown in Figure 6. In this embodiment only one encrypted session key is transmitted to all users. All users employ the same distribution key D but its derivation for each subscriber is unique. The distribution key D is derived from a fixed key K and a subscriber code C. Block 50 represents the received digital data channel of the television signal which includes the encrypted session key and the encrypted video descramble code. The encrypted session key is provided to block 54 where the fixed key K is maintained secret. The subscriber code C from block 51 is also unique to the subscriber and is entered manually by the subscriber. The advantage of this system is that only one encrypted session key has to be transmitted. The sessions can, therefore, be brief. Moreover, the distribution key D can be changed at infrequent intervals by updating the manual input code C. Distribution key D is derived from fixed key K and subscriber code C in block 52. The encrypted session key is thus decrypted in block 54 by the derived distribution key D and is supplied to block 55 along with the encrypted descrambling code from the data channel. The descrambling code is decrypted in block 55 by the now decrypted session key and is then available for descrambling or decrypting signals in the receiver as represented by blocks 56, 57 and 58.

A further embodiment of the present invention with respect to decryption at the receiver end is shown in Figure 7. This embodiment eliminates the need for manual input of a code by the subscriber and

the existence of a common distribution key for all subscribers. In this embodiment, the data channel of the signal includes the encrypted session key, a unique validation code based on the decoder's address or serial number and the encrypted descrambling code. The session key is provided to block 62 where it is decrypted by a distribution key from block 61. The decrypted encryption key is then provided to block 64 where a unique 32 bit internal validation code is derived based on the session key and the address or serial number of the decoder. The derived validation code is compared to the validation code transmitted in the data channel and if the two match, a logic signal is provided to AND gate 66. AND gate 66 allows the decrypted session keys from block 62 to pass through to block 67 only when the derived internal validation code matches the validation code transmitted in the data channel. The session key may then be used by block 67 to decrypt the descrambling code.

In the embodiment shown in Figure 7, every session is 30 seconds in duration and within this period, every decoder decrypts the session key for the next session. The session key is derived within a custom integrated circuit as indicated by reference number 62 in Figure 7 which is very difficult to copy. The session key currently being used to decrypt the video descrambling codes in the data channel is also employed to derive the internal validation code. Single-bit error correction is applied to the received validation codes which are 32-bits in length (sufficient to address up to 4 billion decoders). The session key is released from the custom IC only if an appropriate validation code has been received some time during the last 7 hours of operation on any particular television channel.

The validation codes (with error correction bits) comprise a 39 bit word, these being transmitted in a 250 Kb/s channel. Twenty million receivers are thereby addressable within each 52 minute period. Over a period of 7 hours, each decoder will be validated on 8 separate occasions with a single-error corrected code. With a BER of

10-2, failure of validation at each attempt would occur with probability 0.044. Failure on all eight attempts would occur with a probability 1.4 x 10-11 (MTBF 100 million years).

The great advantage of validation codes is that (unlike session keys) they can be received incorrectly for much of the time without affecting service to the customer. Therefore they do not require extensive error correction. In a field of 10 million receivers, the address cycle time is 26 minutes. If most decoders were operating at 10-3 BER, then 99.95% of the decoders would be validated within the normal transmission time of a typical TV program.

With the embodiment shown in Figure 7, the television receiver should automatically switch between commonly used channels to gather validation codes when in standby operation. However, standby operation is not a mandatory requirement provided that session counts (since the last validation) are stored (within the secure IC) in non-violatile memory, and that the receiver is operational for at least one continuous period of 52 minutes during each 7 hour period of use. As an alternative, the receiver can keep track of operational periods and extend the 7 hour limit to an arbitrary maximum to ensure a predetermined probability of receiving a validation code. Additionally the receiver could issue messages (via teletext display) requesting a period of operation or standby mode when (according to its counters) only one hour of validation remains. Finally, at the end of the 7 hour period, the receiver need not turn off the service completely, i.e., stop descrambling the signal, but, instead, initiate a period of decreasing service, as for example, starting with several hours of monochrome reception. Numerous possibilities exist to encourage payment of subscriptions and/or operation to ensure receipt of validation codes. The function of the validation codes is to allow the receiver to 'form a view' concerning the validity of reception for each of the channels in use. The receiver should act intelligently to gather the necessary evidence for its decision, and take action only when sufficient evidence is at hand.

In the embodiment shown in Figure 7, within 10 seconds of being switched on (or immediately if in standby mode) the security device has decrypted the session key for the next session. This key will not be released unless the receiver is currently validated, but derivation of the session key occurs independently of the validation process. If it were possible to break the security of the integrated circuit performing this function, it would become feasible to design an alternative circuit which did not require validation, and which released the session key unconditionally.

Although security devices now exist which are extremely difficult to copy, a potential security risk is apparent, and a scheme has been designed for its avoidance. Any device designed to deliver session keys, with or without validation, must make use of the distribution keys D (presumably acquired by breaking into one of the security devices). If pirate receivers are discovered which contain particular distribution keys, the corresponding session key encryptions may be excluded from the key distribution channel on condition that all other decoders are left with at least at one key (D) capable of decrypting session keys. This can be arranged by providing each decoder with four keys selected from the 3,000, no two decoders having the same set of four keys. There are 3.3×10^{12} ways of selecting four different keys from 3,000. All copies of any single decoder can be eliminated by the exclusion of its four encrypted session keys, leaving all others (of the 20 million) operational. If a second decoder is copied, all copies can be again disabled at zero cost. Up to ten decoders can be eliminated in this manner. Thereafter, further exclusions will cause some legal decoders to become disabled. These decoders (and the customers who own them) can be predicted through software at the transmitter end. To simultaneously disable all copies of 20 different decoders in a field of 20 million would require replacement of only 10 legal decoders.

With reference to Figure 8, a block diagram is provided showing one example of a decoder which can be used to implement the present invention. A further example of such a decoder is described in commonly assigned U.S. Patent Application Serial No. 507,565 entitled "Encryption and Decryption of Video Signals" filed June 24, 1983 and which is incorporated herein by reference.

As shown in Figure 8, a scrambled MAC television signal first enters a multiplexer 300, which separates from it the luminance and chrominance signals (i.e., the color components), as well as the audio, synchronization, timing and any teletext information. The luminance signal is delivered to luminance store 302, a CCD line store, where it is decompressed, and then to low-pass filter 304, where it is filtered. The analog luminance signal then goes to output interface 306. The sampling signals necessary to decompress luminance are produced in timing generator 308 and supplied to luminance store 302 by two clock drivers 310.

The chrominance signal from demultiplexer 300 is also decompressed in chrominance store 312, which is also a CCD line store. Separate outputs are provided for the two color difference signals, which are filtered in two low-pass filters 314 and then supplied to output interface 306. The necessary sampling signals are supplied to chrominance store 312 from timing generator 308 through three clock drivers 310.

Signals not constituting luminance or chrominance are also separated from the MAC television signal by demultiplexer 300. These signals include audio, teletext and synchronization signals which are delivered to demultiplexer 316 through one of two low-pass filters 318; while the fixed-frequency timing information is delivered to demultiplexer 316 through band-pass filter 320. Demultiplexer 316 separates these signals, supplying the audio to audio demultiplexer 322 and the synchronization and timing signals to clock and synchronization recovery circuit 324 and timing generator 308. Audio information from

demultiplexer 316 is separated into four channels in audio demultiplexer 322 and output by analog audio processor 326. Teletext information is sent to character generator 328 via clock and synchronization recovery circuitry 324. Decoder operations are under the control of microprocessor 330, which communicates with clock and synchronization recovery circuit 324, teletext character generator 328, and RAM 332 over bidirectional buses 334, 336 and 338.

Output interface 306 receives teletext characters from character generator 326, luminance from low-pass filter 304, chrominance from low-pass filters 314, and timing signals from timing generator 308. Its output is a standard NTSC color television signal for display on a television receiver.

The present invention has been described in detail in connection with preferred embodiments. These embodiments, however, are merely examples and the invention is not restricted thereto. It will be understood by those skilled in the art from a reading of the specification that variations and modifications can be made within the scope of the present invention as defined by the appended claims.

CLAIMS

1. An apparatus for encrypting a code for descrambling and/or decrypting information, said apparatus comprising:

first encryption key means for providing a first encryption key;

second encryption key means for providing a second encryption key;

first encryption means for encrypting said second encryption key in accordance with said first encryption key;

second encryption means for encrypting said code in accordance with said second encryption key, said encrypted second encryption key and said encrypted code being provided for descrambling and/or decrypting said information.

2. The apparatus of claim 1 wherein said information is the intelligence portion of a television signal.

3. The apparatus of claim 2 wherein said code includes a plurality of keys for descrambling and/or decrypting said intelligence portion of said television signal.

4. The apparatus of claim 2 further comprising transmission means for transmitting said encrypted second encryption key and said encrypted code to a receiver which receives said television signal.

5. The apparatus of claim 4 wherein said transmission means is the television transmitter which transmits said television signal.

6. The apparatus of claim 1 wherein said code is periodically changed.

7. The apparatus of claim 1 wherein said first encryption key is periodically changed.

8. An apparatus for decrypting a code for descrambling and/or decrypting information, wherein said code is encrypted in accordance with an encrypted first encryption key, said apparatus comprising:

decryption key means for providing a first decryption key;

first decryption means for decrypting said encrypted encryption key in accordance with said decryption key;

second decryption means for decrypting said code in accordance with said encryption key for descrambling and/or decrypting said information.

9. The apparatus of claim 8 wherein said information is the intelligence portion of a television signal.

10. The apparatus of claim 9 wherein said code includes a plurality of keys for descrambling and/or decrypting said intelligence portion of said television signal.

11. A system for encrypting a code for descrambling and/or decrypting information and for decrypting said code, said system comprising:

first encryption key means for providing a first encryption key;

second encryption key means for providing a second encryption key;

first encryption means for encrypting said second encryption key in accordance with said first encryption key;

second encryption means for encrypting said code in accordance with said second encryption key;

first decryption key means for providing a first decryption key;

first decryption means for decrypting said encrypted second encryption key in accordance with said first decryption key;

second decryption means for decrypting said code in accordance with said second decryption key for descrambling and/or decrypting said information.

12. The apparatus of claim 11 wherein said information is the intelligence portion of a television signal.

13. The apparatus of claim 12 wherein said code includes a plurality of keys for descrambling and/or decrypting said intelligence portion of said television signal.

14. The apparatus of claim 12 further comprising transmission means for transmitting said encrypted second encryption key and said encrypted code to a receiver which receives said television signal.

15. The apparatus of claim 14 wherein said transmission means is the television transmitter which transmits said television signal.

16. The apparatus of claim 11 wherein said code is periodically changed.

17. The apparatus of claim 11 wherein said first encryption key is periodically changed.

18. A method for encrypting a code for descrambling and/or decrypting information, said method comprising the steps of:

providing a first encryption key;

providing a second encryption key;

encrypting said second encryption key in accordance with said first encryption key; and

encrypting said code in accordance with said second encryption key, said encrypted second encryption key and said encrypted code being provided for descrambling and/or decrypting said information.

19. The method of claim 18 further including the step of transmitting said encrypted second encryption key and said encrypted code to a receiver which receives said television signal.

20. The method of claim 18 further including the step of periodically changing said code.

21. The method of claim 18 further including the step of periodically changing said first encryption key.

22. A method for decrypting a code for descrambling and/or decrypting information, wherein said code is encrypted in accordance with an encrypted first encryption key, said method comprising the steps of:

providing a decryption key;

decrypting said encrypted first encryption key in accordance with said first decryption key;

decrypting said code in accordance with said first encryption key for descrambling and/or decrypting said information.

23. A method for scrambling and descrambling a line-scanned television signal of the type wherein in each line there is a first period during which video information is present and a second period during which no video information is present, said method comprising the steps of:

scrambling said video information in accordance with video scrambling codes;

providing video descrambling codes for descrambling said scrambled video information;

encrypting said video descrambling codes in accordance with a first encryption key;

providing a session key for decrypting said encrypted video descrambling codes;

encrypting said session key in accordance with a second encryption key;

including said encrypted video descrambling codes and said encrypted session key in said television signal during said second period during which no video information is present; and

providing a distributing key at the receiver which receives said television signal, said distribution key being provided to decrypt said encrypted session key, said decrypted session key being used to decrypt said encrypted video descramble codes, said decrypted video descramble codes being used to descramble said scrambled video information.

24. The method of claim 23 wherein said step of providing a session key includes the step of deriving said session key from said first encryption key.

25. The method of claim 1 wherein the step of providing a distribution key at said receiver includes the step of deriving said distribution key from said second encryption key.

26. The method of claim 23 wherein said step of providing at least one session key includes the step of providing a unique session key for each of said receivers which receive said television signal.

27. The method of claim 4 wherein the step of providing a distribution key includes the step of providing a distribution key for each of said unique session key.

28. The method of claim 1 wherein said session key and said distribution key are changed periodically.

29. A method for scrambling and unscrambling a line-scanned television signal of the type wherein in each line there is a first period during which video information is present and a second period during which no video information is present, said method comprising the steps of:

scrambling said video information in accordance with video scrambling codes;

providing video descrambling codes for descrambling said scrambled video information;

encrypting said video descrambling codes in accordance with a first encryption key;

providing a session key for decrypting said encrypted video descrambling codes;

encrypting said session key in accordance with a second encryption key;

including said encrypted video descrambling codes and said encrypted session key in said television during said second period during which no video information is present; and

providing a subscriber code and a fixed key at the receiver which receives said television signal, said subscriber code and said fixed key being used to derive a distribution key, said distribution

key being used to decrypt said encrypted session key, said decrypted session key being used to decrypt said encrypted video descramble codes, said decrypted video descramble codes being used to descramble said scrambled video information.

30. The method of claim 29 wherein said step of providing a session key includes the step of deriving said session key from said first encryption key.

31. The method of claim 29 wherein said session key is changed periodically.

32. The method of claim 29 wherein the step of providing a subscriber code and a fixed key includes the step of providing a unique subscriber code for each of said receivers which receive said television signal.

33. A method for scrambling and unscrambling a line-scanned television signal of the type wherein in each line there is a first period during which video information is present and a second period during which no video information is present, said method comprising the steps of:

scrambling said video information in accordance with video scrambling codes;

providing video descrambling codes for descrambling said scrambled video information;

encrypting said video descrambling codes in accordance with a first encryption key;

providing a plurality of validation codes, each of said plurality of validation codes being unique for each of said receivers which receives said television signal;

encrypting said session key in accordance with a second encryption key;

transmitting said encrypted video descrambling codes, said encrypted session key and said plurality of validation codes during said second period in said television signal during which no video information is present; and

providing a distribution key at the receiver which receives said television signal, said distribution key being provided to decrypt said encrypted session key, said decrypted session key being used to derive an internal validation code within each of said receivers, said internally derived validation code being compared with said plurality of validation codes, said comparator providing a logic signal indication when a match is found, said logic signal enabling logic means to permit said decrypted session key to decrypt said encrypted video descramble codes, said decrypted video descramble codes being used to descramble said scrambled video information.

34. The method of claim 33 wherein said step of providing a session key for decrypting said encrypted video descrambling codes includes the step of deriving said session key from said first encryption key.

35. The method of claim 33 wherein the step of providing a distribution key at said receiver includes the step of deriving said distribution key from said encryption key.

36. The method of claim 33 wherein the step of providing a distribution key at the receiver includes the step of providing a distribution key which matches said unique session key for each of said receivers.

37. The method of claim 33 wherein said session key and said distribution keys are changed periodically.

FIG. 1

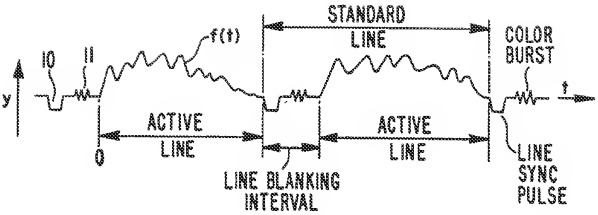


FIG. 2

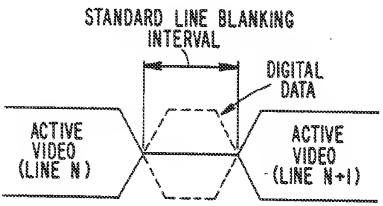
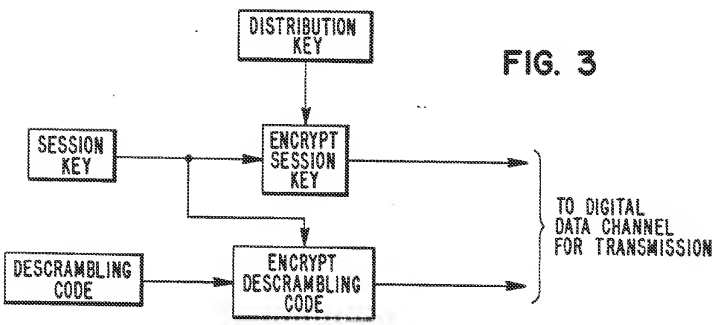


FIG. 3



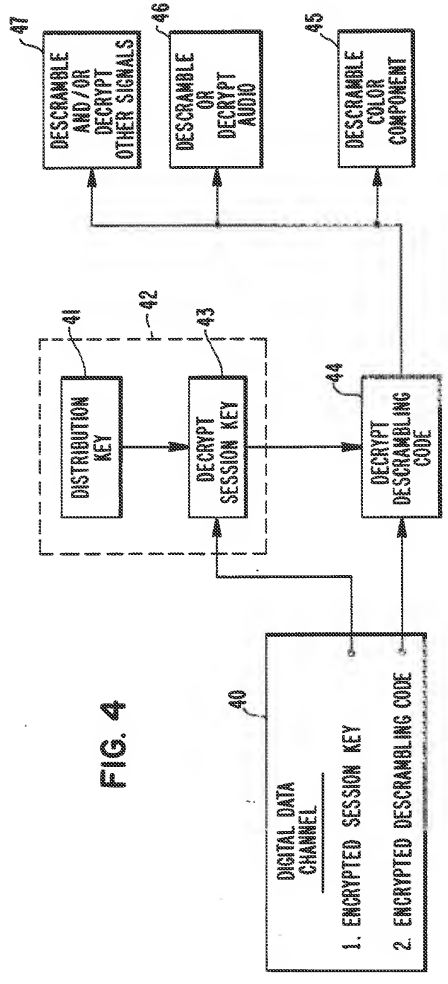

47
DESCRAMBLE AND/OR DECRYPT OTHER SIGNALS
46
DESCRAMBLE OR DECRYPT AUDIO
45
DESCRAMBLE COLOR COMPONENT
41
42
43
44
DISTRIBUTION KEY
DECRYPT SESSION KEY
DECRYPT DESCRAMBLING CODE
40
DIGITAL DATA CHANNEL
1. ENCRYPTED SESSION KEY
2. ENCRYPTED DESCRAMBLING CODE

FIG. 4

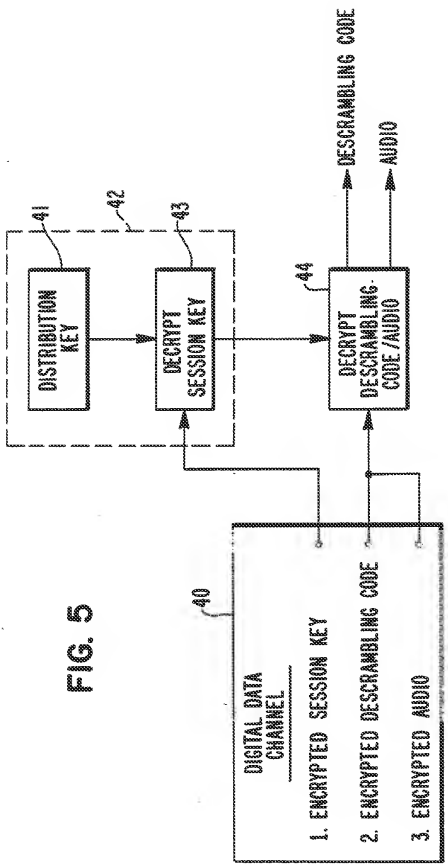

DESCRAMBLING CODE
AUDIO
41
42
43
44
DISTRIBUTION KEY
DECRYPT SESSION KEY
DECRYPT DESCRAMBLING CODE/AUDIO
40
DIGITAL DATA CHANNEL
1. ENCRYPTED SESSION KEY
2. ENCRYPTED DESCRAMBLING CODE
3. ENCRYPTED AUDIO

FIG. 5

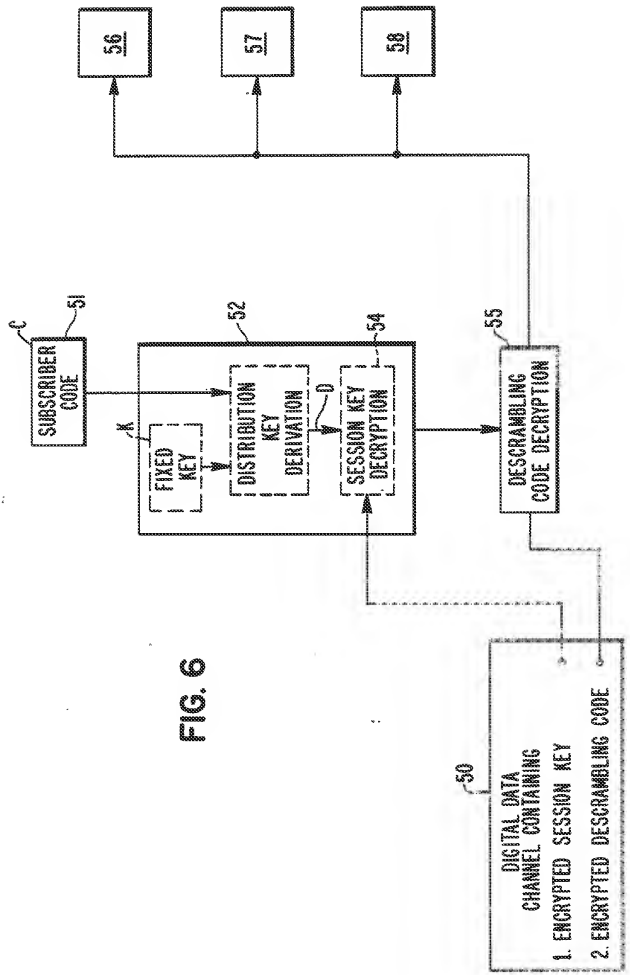
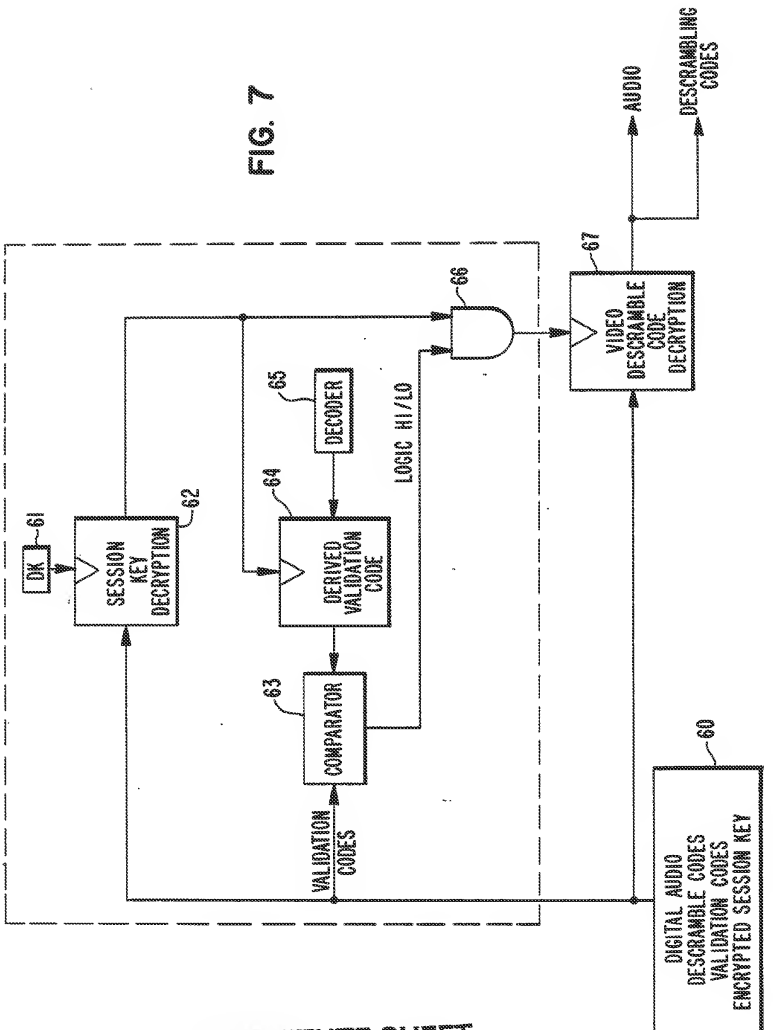

56
57
58
C
51
SUBSCRIBER CODE
52
54
55
K
FIXED KEY
DISTRIBUTION KEY DERIVATION
D
SESSION KEY DECRYPTION
DESCRAMBLING CODE DECRYPTION
50
DIGITAL DATA CHANNEL CONTAINING
1. ENCRYPTED SESSION KEY
2. ENCRYPTED DESCRAMBLING CODE

FIG. 6

FIG. 7


DIGITAL AUDIO
DESCRAMBLE CODES
VALIDATION CODES
ENCRYPTED SESSION KEY
60
VALIDATION CODES
COMPARATOR
63
DERIVED VALIDATION CODE
64
DECODER
65
LOGIC HI/LO
66
DK
61
SESSION KEY DECRYPTION
62
VIDEO DESCRAMBLE CODE DECRYPTION
67
AUDIO
DESCRAMBLING CODES

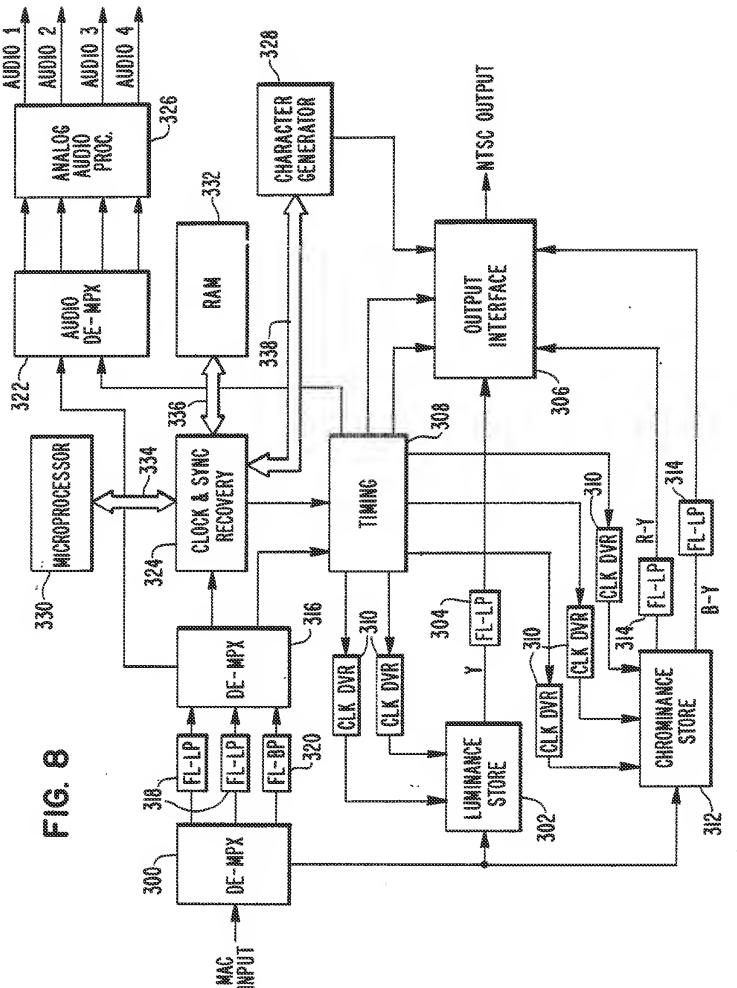

MAC INPUT
DE-MPX
FL-LP
FL-LP
FL-BP
DE-MPX
CLK DVR
CLK DVR
LUMINANCE STORE
FL-LP
Y
CLK DVR
CLK DVR
CHROMINANCE STORE
R-Y
FL-LP
B-Y
FL-LP
TIMING
CLOCK & SYNC RECOVERY
MICROPROCESSOR
AUDIO DE-MPX
ANALOG AUDIO PROC.
AUDIO 1
AUDIO 2
AUDIO 3
AUDIO 4
RAM
CHARACTER GENERATOR
OUTPUT INTERFACE
NTSC OUTPUT
300
302
304
306
308
310
312
314
316
318
320
322
324
326
328
330
332
334
336
338

FIG. 8

INTERNATIONAL SEARCH REPORT

International Application No PCT/US86/00801

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [3]

According to International Patent Classification (IPC) or to both National Classification and IPC

INT. CL 4 H04N 7/167; H04L 9/00
U.S. CL. 358/122, 123; 178/22.15, 22.13, 22.16

II. FIELDS SEARCHED

Minimum Documentation Searched [4]

Classification System	Classification Symbols
US	358/122, 123, 114 178/22.08, 22.09, 22.13, 22.14, 22.15, 22.16

Documentation Searched other than Minimum Documentation to the Extent that such Documents are included in the Fields Searched [5]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [14]

Category *	Citation of Document, [16] with indication, where appropriate, of the relevant passages [17]	Relevant to Claim No. [18]
X	US,A, 4,484,027 (LEE ET AL) 20 November 1984, See Col 3, line 17-Col 4, line 10	1-37
Y,P	US,A, 4,531,020 (WECSELBERGER ET AL) 23 July 1985, See Col 2, lines 3-36	1-37
Y	US,A, 4,388,643, (AMINETZAH) 14 June 1983 See Col 2, lines 18-57	1-37

* Special categories of cited documents: [15]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search [2]	Date of Mailing of this International Search Report [2]
20 May 1986	17 JUL 1986
International Searching Authority [1]	Signature of Authorized Officer [20]
ISA/US	Melissa L. Koltak Melissa Koltak

Form PCT/ISA/210 (second sheet) (Octobsr 1981)

Web Images Video News Maps more »

Google scholar "public key" "conditional access" - 2001 Searc

Search only in Engineering, Computer Science, and Mathematics.
Search in all subject areas.

Scholar **All articles** - Recent articles Results 1 - 100 of about 164 for "public key" "conditional acc

[PDF] Smart cards and **conditional access**
LC Guillou, ... - Advances in Cryptography—Proceedings of EuroCrypt, 1985 - zedz.net
... 4 - A CP8 CARI FOR **CONDITIONAL ACCESS** **Conditional access** key carrier cards are now ...
TOWAEPS DIGITAL SIGNATURES Secret functions of a **public key** cryptosystem can ...
Cited by 37 - Related articles - Web Search - All 2 versions

Cryptology for digital TV broadcasting
BM Macq, JJ Quisquater - Proceedings of the IEEE, 1995 - ieeexplore.ieee.org
... The **conditional access**, ie, the scrambling key distribution system, is discussed
in Section III. ... K1 in (I), is seen as a **public key** (everyone is able to encrypt ...
Cited by 206 - Related articles - Web Search - BL Direct - All 2 versions

Method and apparatus for providing **conditional access** in connection-oriented interactive networks ...
AH Wasilewski, DF Woodhead, GL Logston - US Patent App. 09/135,615, 1998 - Google Patents
... Methods and apparatus for applying **conditional access** are described that comprise
encrypting ... encrypting the second key according to a **public-key** encryp- tion ...
Cited by 31 - Related articles - Web Search - All 7 versions

Digital rights management and watermarking of multimedia content for m-commerce applications
F Hartung, F Ramme - IEEE Communications Magazine, 2000 - ieeexplore.ieee.org
... Encryption **Conditional access** Copy control Identification and tracing ... The DRM system
also includes a **public key** decryp- tion engine, a block cipher for bulk ...
Cited by 120 - Related articles - Web Search - BL Direct - All 6 versions

Method for securely distributing a conditional use private key to a trusted entity on a remote ...
GL Graunke, J Carbajal, RL Maliszewski, CV Rozas - US Patent 6,901,393, 1999 - Google Patents
... such as a DVD player or CD-ROM player) with **conditional access** based on ... MANIFEST
WITH ASYMMETRIC PRIVATE KEY AND STORE CORRESPONDING ASYMMETRIC **PUBLIC KEY** IN A ...
Cited by 24 - Related articles - Web Search - All 2 versions

The ESPRIT Project CAFE—High Security Digital Payment Systems— kuleuven.ac.be
[PDF]
JP Boly, A Bosselaers, R Cramer, R Michelsen, S ... - Computer Security-ESORICS 94: Third European Symposium on ..., 1994 - books.google.com
... A Method for Obtaining Digital Signatures and **Public- Key** Cryptosystems; Communications
of ... Waid 94 Michael Waidner: CAFE-**Conditional Access** for Europe; 4. GMD ...
Cited by 116 - Related articles - Web Search - BL Direct - All 28 versions

An overview of multimedia content protection in consumer electronics devices- cuny.edu
[PDF]
AM Eskicioglu, EJ Delp - Signal Processing: Image Communication, 2001 - Elsevier
... Both symmetric and **public key** ciphers are commonlyused for content ... Such architectures
are considered extensions of **conditional access** systems, restricting ...